UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,949	08/08/2006	David Arditti	33901-219PUS	2791

27799 7590 09/19/2008

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/588,949	ARDITTI ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☒ Claim(s) *1-9* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8-8-06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/588949 filed on 8/8/06 is presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Information Disclosure Statement

The information disclosure statement filed 8-8-06 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; **each non-patent literature publication or that portion which caused it to be listed**; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered. A copy of the non-patent literature of Menezes has not been received by the Office.

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the method of claims 1-7, specifically the manipulation of the data and keys must be shown or the feature(s)

canceled from the claim(s). Furthermore, nothing of the authentication method of claim 2 is disclosed in the drawings as well. No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claims 1-9 are objected to because of the following informalities:

Claim 1 lacks antecedent basis for "that public key", "the public key", “the terminal”, and “the network entity”. References to entities should use the same exact wording (i.e. the mobile terminal, the telecommunications network entity).

The rest of the claims have similar informalities with respect to the network entity and the terminal.

Each of the dependent claims (2-7) should be written to incorporate all the limitations of the parent claim. As such the dependent claims should reference their parent claim by "the" method or "the" device, not "a" method or "a" device. Use of "the" removes any doubt as to whether the method (or device) is the same method of its parent and not a similar method.

Claim 3, recites the phrase "with a view" but this is an awkward phrase probably resulting in translation from a foreign language. Examiner suggests a less literal translation.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 8, the limitation "means in the mobile terminal for generating a public key" invokes 35 USC 112 6th paragraph. In searching the specification for adequate structure, material, or acts for performing the recited function, none could be found. The written description merely discloses that the mobile terminal generates a key pair (private/public). In the art, key generation can be accomplished in so many ways, some of which require user input, others do not. Even though the specification discloses the known method of authentication in a GSM network it is unclear whether or not the applicant is uses this method to obtain the key pair. In the known GSM method, the key pair is stored on the SIM at time of manufacturing. However, the claim language for obtaining the key pair is generating. Generating implies some type of calculation or computation to derive a key from some other data. If Applicant is intending the disclosure of the known GSM system to provide adequate structure, material, or acts for performing key pair generation, he should state that on the record. Also, with that intention, a more suitable word than generating could be used to make the invention clearer. Appropriate correction is required.

Claim 8 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession

of the claimed invention. For the reasons listed above, claim 8 fails to provide the written description support for generating a key.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 9, the limitation "means for producing at least one key for decrypting messages received by the terminal" invokes 35 USC 112 6th paragraph. In searching the specification for adequate structure, material, or acts for performing the recited function, none could be found. The written description merely discloses that the mobile terminal generates a key pair (private/public). In the art, key generation can be accomplished in so many ways, some of which require user input, others do not. Even though the specification discloses the known method of authentication in a GSM network it is unclear whether or not the applicant is uses this method to obtain the key pair. In the known GSM method, the key pair is stored on the SIM at time of manufacturing. However, on page 8, lines 23-26 of the specification, Applicant says the key pair is generated in the phone. It is also unclear from the context of the specification whether or not the Applicant's invention uses the GSM authentication method. It appears Applicants intends on simplifying that method on page 9, starting on line 11. Again, Applicant discloses generating a key pair. If Applicant is intending the disclosure of the known GSM system to provide adequate structure, material, or acts for performing key pair generation, he should state that on the record.

Furthermore, claim 9 discloses producing a key for decrypting messages received by the terminal. The key for decrypting messages received would be a private key. However, claim 9, then discloses this "said key" is sent to the certification authority so that it can become a public key. This goes against the philosophy of asymmetrical keys. One does not publish the key (private) for decrypting. It is the public key which is used as the encryption key that is published.

Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. For the reasons listed above, claim 9 fails to provide the written description support for generating a key.

Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. For the reason mentioned above in relation to publishing the private key, the claim matter does not enable proper encryption for which the invention is described in the specification.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 9 is rejected under 35 U.S.C. 102(b) as being anticipated by USP 6,772,331 to Hind et al., hereinafter Hind.

As per claim 9, Hind teaches a mobile telecommunications terminal, comprising: means for producing at least one key for decrypting messages received by the terminal (col. 9, lines 65-67); and

means for sending said key to a certification authority by means of a network call via a telephone network entity so that said key becomes a public key (col. 10, lines 5-10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind in view of USP Application Publication 2003/0210789 to Farnham et al., hereinafter Farnham.

As per claim 1, Hind teaches a certification method using a public key certification authority and involving at least one mobile terminal able to receive messages encrypted by that public key, wherein the method comprises:

the step of the mobile terminal generating the public key (col. 9, lines 65-67);

the step of a telecommunications network entity acquiring said key from the terminal by means of a network call (col. 10, lines 3-5); and

the step of supplying the certification authority with the public key and the associated result of the authentication process (col. 10, lines 5-10).

Hind teaches that the mobile terminal creates an encrypted session with the network entity. Hind also teaches various key agreements between devices which already have a certification (col. 10, lines 30-65). However, Hind does not explicitly teach that the mobile terminal authenticates itself to the network entity prior to the certification. Farnham teaches a process by which the network entity authenticates the terminal by a party authentication process used in relation to a standard telephone call (0014). Authentication is well known in the art and anyone of ordinary skill in computer security knows the importance of it. Combining the authentication method of Farnham which is very similar to the encryption method taught by Hind further strengthens the protocol. Farnham provides motivation for his authentication scheme as it eliminates a man-in-the-middle attack. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the authentication of the mobile terminal with the teaching of Hind to prevent an attacker from impersonating the mobile terminal.

As per claim 2, Hind does not explicitly teaches the authentication method of the mobile terminal includes the mobile terminal sending a calculation result involving a confidential key stored in the mobile terminal and the step of the network entity comparing the result with an expected result also calculated by the network entity using the same confidential key, a positive comparison result being interpreted as an identification of the mobile terminal. This authentication step is a Diffie Hellman key exchange. Hind does teach a Diffie Hellman key exchange as a way to form a session key (col. 10, lines 40-42). Farnham takes this a step further by using the public key of terminal as a means to authenticate the terminal to the server (0014). Examiner supplies the same rationale for combining Hind with Farnham as being obvious to one of ordinary skill in the art at the time of the invention.

As per claim 3, Hind does not explicitly teach the step of the network entity sending random data to the terminal and the step of the terminal calculating the random data sent by the network entity, the step of calculation by the network entity also involving said random data with a view to said comparison of results. Farnham teaches the step of the network entity sending random data to the terminal and the step of the terminal calculating the random data sent by the network entity, the step of calculation by the network entity also involving said random data with a view to said comparison of results (0014). Use of random data in an authentication protocol is both well known and taught by Farnham as a means to prevent replay attacks in securing a channel. Therefore it would have been obvious to one of ordinary skill in the art at the time of the

invention to use the random data in the authentication protocol to increase the difficulty in comprising the system.

As per claim 4, Hind teaches the step of the mobile terminal generating, in addition to the public key, a confidential key held in memory in the mobile terminal and used to decrypt received messages that were encrypted with the public key (col. 9, line 64).

As per claim 5, Hind teaches the terminal is adapted to send messages and to append to them an authentication signature produced using the confidential key that it previously generated itself (col. 11, lines 33-35).

As per claim 6, Hind teaches the step of the network entity sending the public key to the certification authority via a channel that is secured against unauthorized reading (col. 9, lines 37-39).

As per claim 7, Hind teaches the step of the mobile terminal using an authentication key of the mobile terminal usually employed in relation to telephone calls, generating an encryption key, encrypting messages using that encryption key and sending said messages (col. 10, lines 40-50).

As per claim 8, Hind teaches a mobile telecommunications system comprising:
at least one mobile terminal (col. 9, lines 66-67);
one network entity [administration server] (col. 10, lines 4-5);

means in the mobile terminal for generating a public key (col. 9, lines 66-67);
means in the telecommunications network entity for acquiring said public key from the mobile terminal by means of a network call (col. 10, lines 3-5);

a certification authority [CA] (col. 10, lines 9-10); and

means for supplying the certification authority with the public key generated by the mobile terminal and the associated result of the authentication process (col. 10, lines 9-10). Hind teaches that the mobile terminal creates an encrypted session with the network entity. Hind also teaches various key agreements between devices which already have a certification (col. 10, lines 30-65). However, Hind does not explicitly teach that the mobile terminal authenticates itself to the network entity prior to the certification. Farnham teaches a process by which the network entity authenticates the terminal by a party authentication process used in relation to a standard telephone call (0014). Authentication is well known in the art and anyone of ordinary skill in computer security knows the importance of it. Combining the authentication method of Farnham which is very similar to the encryption method taught by Hind further strengthens the protocol. Farnham provides motivation for his authentication scheme as it eliminates a man-in-the-middle attack. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the authentication of the mobile terminal with the teaching of Hind to prevent an attacker from impersonating the mobile terminal.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

USP Application Publication 2002/0118674 discloses a Diffie Hellman key exchanging method for mobile networks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2131

/Syed Zia/

Primary Examiner, Art Unit 2131